2019年1月31日

NEWS RELEASE

キヤノンマーケティングジャパン株式会社

2018年12月のマルウェアレポートを公開
～12種類の新たなLinuxのOpenSSHバックドアをESET社が発見～

キヤノンマーケティングジャパン株式会社（代表取締役社長：坂田正弘、以下キヤノンMJ）は、2018年12月のマルウェア検出状況に関するレポートを公開しました。世界全体で最も多く検出された不正広告スクリプトや、新たに発見された12種類のLinuxのOpenSSHバックドアなどについて解説しています。

■ 2018年12月のマルウェア検出状況に関するレポートを公開

キヤノンMJのマルウェアラボでは、国内で利用されているウイルス対策ソフトウェア「ESETセキュリティ ソフトウェア シリーズ」のマルウェア検出データを基に、2018年12月のマルウェア検出状況を分析し、レポートを公開しました。

2018年12月のマルウェア検出状況に関するレポート
【 https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1812.html 】

■ トピック

・12月の概況：不正広告スクリプトの検出数が国内に加え世界全体で最多

12月に国内と世界全体で最も多く検出されたマルウェアは、Web閲覧中に不正広告を表示させる可能性があるスクリプトであるJS/Adware.Agentでした。数多くの攻撃者が不正広告を利用した収益に対して継続的に関心を示していることが考えられます。

12月の国内マルウェア検出数上位10件のうち8件がWeb上で動作するなど、前月に続き今月もWeb上で動作するマルウェアが多く検出されました。Web上で動作するマルウェアは、OSの種類やプラットフォームに関係なくあらゆる環境で動作が可能なため汎用性があります。

・12種類の新たなLinuxのOpenSSHバックドアを発見

ESET社が2018年12月に公表した21種類のLinuxバックドアの解析結果のうち12種類はこれまで詳細が知られていなかった新しいバックドアでした。バックドアは「裏口」を意味するマルウェアで、攻撃者がシステムに侵入した際、次回以降侵入しやすくする目的で設置され、感染した場合、情報が窃取されるほか感染端末を不正行為の踏み台として使われる恐れがあります。

今回公表されたバックドアはすべてOpenSSHを基に作成されています。OpenSSHは、無償でソースコードを入手できるため、改変（バックドア化）がしやすく隠密に攻撃活動を行えることなどから攻撃者に好まれると考えられます。

マルウェアレポート内では、特徴的なバックドアChandrila、Bonadan、Kessel、Kaminoの4種類について解説しています。

● 一般の方のお問い合わせ先 ：ESETサポートセンター　050－3786－2528
● ニュースリリースホームページ ：canon.jp/newsrelease ● ESETホームページ：https://eset-info.canon-its.jp/

■ 12月の概況

12月に国内で最も多く検出されたマルウェアは、Web 閲覧中に不正広告を表示させる可能性があるスクリプトである JS/Adware.Agent でした。JS/Adware.Agent は、2018年6月以降、常に国内マルウェア検出数の上位3位以内に含まれ続けています。12月は世界全体においても、本マルウェアが最も多く検出されました。数多くの攻撃者が、不正広告を利用した収益に対して、継続的に関心を示していることが考えられます。

JS/Adware.Agent も含め、今月も Web 上で動作するマルウェアが多く検出されました。12月の国内マルウェア検出数上位10件のうち、8件がWeb 上で動作するものです。Web 上で動作するマルウェアは、OS の種類やプラットフォームに関係なく、あらゆる環境で動作することが可能なため汎用性があります。

■ 12種類の新たな Linux の OpenSSH バックドアを発見

2018年12月5日、ESET 社は21種類の Linux バックドアについて解析結果を公表しました(ESET 社ブログ：https://www.eset.com/us/about/newsroom/press-releases/eset-discovers-12-previously-undetected-linux-backdoors-1/)。このうち12種類は、これまで詳細が知られていなかった新しいバックドアです。

バックドアは「裏口」を意味するマルウェアで、攻撃者がシステムに侵入した際、次回以降侵入しやすくする目的で設置されます。感染した場合、情報が窃取されるほか感染端末を不正行為の踏み台として使われる恐れがあります。

今回公表されたバックドアはすべて OpenSSH を基に作成されています。OpenSSH はオープンソースの SSH (Secure Shell) ソフトウェアで、大抵の Linux ディストリビューションに搭載されていることから一般に広く使われています。

OpenSSH が攻撃者に好まれる理由として、無償でソースコードを入手できるため改変(バックドア化)がしやすいこと、隠密に攻撃活動を行えることなどが考えられます。

マルウェアレポート内では、特徴的なバックドア Chandrila、Bonadan、Kessel、Kamino の4種類について解説しています。

今月も引き続き Web 上で動作するマルウェアが国内で検出されたほか、ESET 社が新たな OpenSSH バックドアを発見しました。常に最新の脅威情報をキャッチアップし、対策を実施していくことが重要です。

■ マルウェアやセキュリティに関する情報を「マルウェア情報局」で公開中

キヤノン MJ では、インターネットをより安全に活用するために、マルウェアや各種セキュリティに関する情報を提供しています。こちらも合わせてご覧ください。

マルウェア情報局
【 https://eset-info.canon-its.jp/malware_info/ 】

マルウェア情報局は、キヤノン MJ が日本国内総販売代理店として取り扱う ESET 製品に関する情報や、マルウェアの情報を提供するポータルサイトです。本サイトでは、スロバキアのセキュリティベンダー ESET 社が発信するニュースを中心に、キヤノン MJ のサイバーセキュリティに関する研究を担うマルウェアラボが発信するレポートを掲載しています。